

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

	X	
In re SONY BMG CD TECHNOLOGIES	:	Civil Action No. 1:05-cv-09575-NRB
LITIGATION	:	
	:	<u>CLASS ACTION</u>
	:	
This Document Relates To:	:	REPLY DECLARATION OF J. ALEX
	:	HALDERMAN IN SUPPORT OF RICCIUTI
ALL ACTIONS.	:	CLASS REPRESENTATIVES' MOTION
	:	FOR AN AWARD OF ATTORNEYS' FEES
	X	AND REIMBURSEMENT OF EXPENSES

I, J. Alex Halderman, hereby declare as follows:

1. I am a Ph.D. candidate in computer science at Princeton University. My research interests include computer security, digital rights management, information privacy, and the interplay between technology and public policy. My advisor is Professor Edward Felten. Along with Professor Felten, I regularly post on the Freedom to Tinker blog, located at: [www.freedom-to-tinker.com](http://www.freedom-to-tinker.com). I have authored, co-authored or assisted in all of the postings on the blog relating to MediaMax DRM software. I have personal knowledge of the matters stated herein, and if called upon, I could and would competently testify thereto.

2. From June 2003 to the present I have been a research assistant at the Princeton University Secure Internet Programming Laboratory. As part of an activate research agenda, I have engaged in projects including denial-of-service defenses for network servers, novel methods for managing user passwords, cryptographic privacy-management techniques for recording devices such as camera phones, and client puzzle approaches to the Sybil attack problem in distributed systems.

3. I have also performed analysis and security evaluation of digital rights management (“DRM”) for audio CDs that has received world-wide media attention.

4. My publications are available online at <http://www.cs.princeton.edu/~jhalderm/papers/>. They include the following:

- (a) Lessons from the Sony CD DRM Episode, with Professor Edward W. Felten;
- (b) Digital Rights Management, Spyware, and Security;
- (c) A Convenient Method for Securely Managing Passwords;
- (d) Privacy Management for Portable Recording Devices;
- (e) New Client Outsourcing Techniques for DoS Protection;
- (f) Analysis of the MediaMax CD3 Copy-Prevention System;

- (g) Early Experiences with a 3D Model Search Engine;
  - (h) A Search Engine for 3D Models; and
  - (i) Evaluating New Copy-Prevention Techniques for Audio CDs.
5. I have received the following awards for my work:
- (a) National Science Foundation Graduate Research Fellowship (2004);
  - (b) Princeton Computer Science Department graduate study award (2003);
  - (c) Princeton Computer Science Department Senior Award (2003);
  - (d) Accenture Prize in Computer Science (2002);
  - (e) Martin A. Dale Summer Award (2000); and
  - (f) Election to honorific societies, including *Phi Beta Kappa* and *Sigma Xi*.

**I. Mr. Jacobson Misstates My Role in the MediaMax 5.0 ACL Problem**

6. Mr. Jacobson's declaration states that over the Thanksgiving holiday, the Freedom to Tinker website indicated a "theoretical" privilege escalation security problem and that EFF subsequently brought that problem to Sony BMG Music Entertainment ("Sony BMG") attention on November 30, 2005. Declaration of Jeffrey S. Jacobson, Esq., in Opposition to the "EFF Group's" Motion for the Award of Attorneys' Fees ("Jacobson Decl."), ¶19. This incorrectly conflates two security problems which are distinct.

7. The privilege escalation security problem, also called an ACL problem, was discovered by Jesse Burns and Alex Stamos of iSEC Security Partners ("iSEC") and is different from the problems that were discussed by Professor Felten and me in late November. iSEC discovered that the MediaMax installer sets file permissions that allow any user to modify its code directory and the files and programs in it. As Burns and Stamos realized, the lax permissions allow a non-privileged user to replace the executable code in the MediaMax player files with malicious code. The next time a user plays a MediaMax-protected CD, the attack code will be executed with that

user's security privileges. The MediaMax player requires Power User or Administrator privileges to run, so it is likely that the attacker's code will run with almost complete control of the system. Normally, this problem could be fixed by manually correcting the errant permissions. However, MediaMax aggressively updates the installed player code each time the software on a protected disc autoruns or is launched manually. As part of this update, the permissions on the installation directory are reset to the insecure state.

8. I first learned about the problem on December 6, 2005, on the day that Electronic Frontier Foundation ("EFF") and Sony BMG made their joint public announcement about the problem and the initial patch to solve it.

9. Professor Felten and I did discover that the initial patch released by Sony BMG on December 6, 2005 in response to the iSec report was capable of triggering precisely the kind of attack it was supposed to prevent. In the process of updating MediaMax, the patch checked the version of MediaMax.dll by invoking executable code within that file. If this file was already modified by an attacker, the process of applying the security patch would execute the attack code. Prior versions of the MediaMax uninstaller had the same vulnerability, though both the uninstaller and the patch have since been replaced with versions that to my knowledge do not suffer from this problem.

10. While Mr. Jacobson notes that the ACL problem discovered by iSEC is a common one, he neglects to point out that the problem is also quite serious. Microsoft has a security management column about it entitled: "How to Shoot Yourself in the Foot with Security, Part 2: To ACL or Not to ACL." <http://www.microsoft.com/technet/community/columns/secmgmt/sm1105.mspx> (November 8, 2005).

**II. My Investigation of MediaMax DRM Revealed Many Other Problems, and Confirmed the Seriousness of the MediaMax 5.0 ACL Problem**

11. Mr. Jacobson asserts that “word” of the ACL problem was posted on the Freedom to Tinker website on November 30, 2005. Jacobson Decl., ¶29. This is not true. The only posting on the website on that day was one noting that Sony BMG had been alerted to the XCP rootkit problem in early October, 2005 and had ignored the alert. Attached hereto as Exhibit 1 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=937>.<sup>1</sup>

12. While I discovered some problems with the MediaMax DRM software in November, 2005, I did not discover or publish the problem that posed the greatest threat to the greatest number of users, which is the ACL problem discovered by iSEC Partners working with EFF. Specifically:

(a) On November 12, 2005, I published a report that MediaMax software installed prior to user consent. Attached hereto as Exhibit 2 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=925>.

(b) On November 17, 2005, I published a report that the uninstaller that Sony BMG created for MediaMax software, in order to allow people to remove the software that had been installed without their consent, itself caused a critical security problem on every computer on which it was used. Professor Felten and I worked with Sony BMG to fix this problem and issue an updated uninstaller. Attached hereto as Exhibit 3 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=931>.

(c) On November 22, 2005, immediately after EFF filed its suit, Professor Felten published a report noting that EFF’s lawsuit correctly focused on MediaMax, unlike the other

---

<sup>1</sup> The complete text of all postings on Freedom to Tinker is available on the website archives and linked from our front page: <http://www.freedom-to-tinker.com>.

litigation. The post stated: “Emphasizing MediaMax seems like a smart move – while Sony has issued an apology of sorts for XCP and has recalled XCP discs, the company is still stonewalling on MediaMax, even though MediaMax raises issues almost as serious as XCP.” Attached hereto as Exhibit 4 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=934>. Note that this posting was prior to the discovery of the ACL problem by iSEC working with EFF. This additional problem made the risk to, and need for relief for MediaMax purchasers even more acute.

(d) On December 7, 2005, after the public announcement of the ACL flaw found by iSEC Partners, I helped Professor Felten write a report about it on the Freedom to Tinker website, including our discovery that the patch created by Sony BMG was defective and required yet another patch to fix. Attached hereto as Exhibit 5 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=942>.

(e) On December 8, 2005, I again assisted Professor Felten in posting about the security flaw discovered by iSEC, in a post entitled: “Not Just Another Buggy Program.” Attached hereto as Exhibit 6 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=944>. The post again emphasizes the seriousness of the security flaw found by iSec and EFF and ends: “Sony is still shipping CDs containing this dangerous software.”

13. Mr. Jacobson’s declaration contains other improper claims as well. For instance, Mr. Jacobson incorrectly asserts that the claims of “spying” by the XCP and MediaMax CDs are unfounded. Jacobson Decl., ¶¶9-10. This is not true. While it is not clear what Sony BMG was doing with the information (Mr. Jacobson refers to a privacy audit that does not appear to be publicly available), it is plain that the software was covertly transmitting usage information back to the Sony BMG or its consultants.

14. In a posting on the website on November 10, 2005, Professor Felten explained why we had come to the conclusion that both the XCP and MediaMax software were spyware. Attached hereto as Exhibit 7 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=923>. The post states:

In all the discussion of the SonyBMG software, I've been avoiding the S-word. But now it's clear that this software crosses the line. It's spyware.

Let's review the evidence:

- The software comes with a EULA which, at the very least, misleads users about what the software does.
- The software interferes with the efforts of ordinary users and programs, including virus checkers and other security software, to identify it.
- Without telling the user or obtaining consent, the software sends information to the vendor about the user's activities.
- No uninstaller is provided with the software, or even on the vendor's website, despite indications to the contrary in the EULA.
- The vendor has an uninstaller but refuses to make it available except to individual users who jump through a long series of hoops.
- The vendor makes misleading statements to the press about the software.

15. Mr. Jacobson also asserts that "several experts now believe that the XCP software does not contain a 'rootkit' as that term is commonly used." Jacobson Decl., ¶7. He does not identify those "experts" or any public statements by them. I am not aware of any security experts who disagree with the broad consensus that the XCP software is a rootkit or at least has significant rootkit-like attributes. In my first post explaining the XCP software on November 2, 2005, I explained why and how it acts like a rootkit, and how the risks it creates for users are the same as those created by many other rootkits. Attached hereto as Exhibit 8 is a true and correct copy of this website posting, found at: <http://www.freedom-to-tinker.com/?p=920>. I stand by that analysis.

16. Additionally, as recently as February of this year, the U.S. Department of Homeland Security has indicated its concern about hidden properties in software programs:

“The recent Sony experience shows us that we need to be thinking about how we ensure that consumers are not surprised by what their software programs do,” Jonathan Frenkel, director of law enforcement policy at the U.S. Department of Homeland Security said in a speech here at the RSA Conference 2006.

Evers, “Homeland Security official suggests outlawing rootkits,” CNET News.com (February 16, 2006), [http://news.com.com/Homeland+Security+official+suggests+outlawing+rootkits/2100-7348\\_3-6040726.html](http://news.com.com/Homeland+Security+official+suggests+outlawing+rootkits/2100-7348_3-6040726.html).

I declare under penalty of perjury under the laws of the State of New York that the foregoing is true and correct. Executed this 12th day of May, 2006, at Princeton, New Jersey.

s/J. Alex Halderman  
\_\_\_\_\_  
J. ALEX HALDERMAN

T:\Cases\SF\Sony NY\DEC00030829.doc

CERTIFICATE OF SERVICE

I hereby certify that on May 12, 2006, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants indicated on the attached Manual Notice List.

/s/ Reed R. Kathrein

REED R. KATHREIN

LERACH COUGHLIN STOIA GELLER

RUDMAN & ROBBINS LLP

655 West Broadway, Suite 1900

San Diego, CA 92101

Telephone: 619/231-1058

619/231-7423 (fax)

E-mail:ReedK@[lerachlaw.com](mailto:ReedK@lerachlaw.com)



## Mailing Information for a Case 1:05-cv-09575-NRB

### Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **Sanford P. Dumain**  
sdumain@milbergweiss.com
- **Jeffrey S. Jacobson**  
jsjacobs@debevoise.com mmgrimes@debevoise.com
- **Scott Adam Kamber**  
skamber@kolaw.com
- **Jonathan K. Levine**  
jkl@girardgibbs.com dcg@girardgibbs.com;ams@girardgibbs.com;ale@girardgibbs.com;  
cme@girardgibbs.com;zml@girardgibbs.com;ajd@girardgibbs.com
- **Ira M. Press**  
ipress@kmslaw.com
- **Shana Eve Scarlett**  
shanas@lerachlaw.com
- **Jason Louis Solotaroff**  
jsolotaroff@gslawny.com
- **Mark A. Strauss**  
mstrauss@kmslaw.com lmorris@kmslaw.com

### Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

**Cindy A. Cohn**

Legal Director of the Electronic Frontier Foundation

454 Shotwell Street  
San Francisco, CA 94110

**Lawrence E. Feldman**

Lawrence E. Feldman & Associates  
432 Tulpehocken Avenue  
Elkins Park, PA 19027

**Jeff D. Friedman**

Lerach Coughlin Stoia Geller Rudman & Robbins LLP  
100 Pine Street  
Suite 2600  
San Francisco, CA 94111

**Daniel C. Girard**

Girard, Gibbs & De Bartolomeo, L.L.P.  
601 California Street  
Suite 1400  
San Francisco, CA 94108

**Robert S. Green**

Green Welling LLP  
595 Market Street  
Suite 2750  
San Francisco, CA 94105

**Reed R. Kathrein**

Lerach Coughlin Stoia Geller Rudman & Robbins LLP  
100 Pine Street  
Suite 2600  
San Francisco, CA 94111

**Elizabeth Pritzker**

Girard, Gibbs & De Bartolomeo, L.L.P.  
601 California Street  
Suite 1400  
San Francisco, CA 94108

**Peter G.A. Safirstein**

Milberg Weiss Bershad & Schulman LLP (NYC)  
One Pennsylvania Plaza  
New York, NY 10119

**Jenelle Welling**

Green Welling LLP

595 Market Street

Suite 2750

San Francisco, CA 94105